UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

OUSSAMA EL OMARI, Plaintiff, v. DECHERT LLP, NICHOLAS PAUL DEL ROSSO, and VITAL MANAGEMENT SERVICES, INC., Defendants.	Civil Action No. 23-cv-04607 (LAK) (OTW)

DEFENDANT DECHERT LLP'S MEMORANDUM OF LAW IN RESPONSE TO PLAINTIFF'S OBJECTIONS TO MAGISTRATE JUDGE WANG'S REPORT AND RECOMMENDATION

Sean Hecker
John C. Quinn
David Gopstein
Mark Weiner
KAPLAN HECKER & FINK LLP
350 Fifth Avenue, 63rd Floor
New York, NY 10118
Tel: (212) 763-0883
Fax: (212) 564-0883
shecker@kaplanhecker.com
jquinn@kaplanhecker.com
dgopstein@kaplanhecker.com
mweiner@kaplanhecker.com

Carmen Iguina González*
KAPLAN HECKER & FINK LLP
1050 K Street NW, Suite 1040
Washington, DC 20001
Tel: (212) 763-0883
Fax: (212) 564-0883
ciguinagonzalez@kaplanhecker.com

**Admitted pro hac vice*

Attorneys for Defendant Dechert LLP

March 21, 2024

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

OTHER AUTHORITIES

Dechert LLP ("Dechert") respectfully submits this Response to Plaintiff's Objection (ECF No. 77) ("Obj.") to the Report and Recommendation of the Honorable Ona T. Wang (ECF No. 76) ("Report" or "R&R"), pursuant to 28 U.S.C. § 636(b) and Rule 72(b) of the Federal Rules of Civil Procedure.[1]

PRELIMINARY STATEMENT

The Court should adopt Judge Wang's well-reasoned Report and Recommendation in full and dismiss Plaintiff's Complaint with prejudice. This is Plaintiff Oussama El Omari's fourth attempt at litigation in seven years (and second against Dechert), all arising from his former employment with an instrumentality of Ras al Khaimah ("RAK"), one of the seven emirates of the United Arab Emirates. The three prior litigations were dismissed at the pleading stage in decisions that were upheld on appeal. As Judge Wang recommended, this new attempt should meet the same fate.

In this iteration, Plaintiff alleges that his emails were hacked so that they could be used in the prior litigations by Dechert, who acted as counsel for the defendants (and itself) in two of those prior cases. More specifically, Plaintiff contends that an Indian hacking firm illegally accessed his email accounts at the direction of Defendants Nicholas Del Rosso and Vital Management Services, who had been engaged as contractors by Dechert in its representations of RAK dating back to 2014. But nowhere in this Complaint does Plaintiff allege that Dechert directed or otherwise contributed to the hacking; indeed, he does not even allege that Dechert was ever provided the purportedly hacked emails. Yet still he accuses Dechert of violating, and conspiring to violate, the Computer Fraud and Abuse Act ("CFAA") and committing conversion under North Carolina state

[1] Plaintiff's 23-page Objection violates Your Honor's Individual Rules providing for a 20-page limit on such objections.

law through this alleged unauthorized access.

As Judge Wang concluded, even assuming the truth of the allegations contained in the Complaint, all of Plaintiff's claims should be dismissed. *First*, Judge Wang correctly determined that the CFAA claims fail because the "loss" Plaintiff maintains he suffered is not actionable under the statute. *See Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021). In addition, Judge Wang properly recognized that the CFAA claims against Dechert fail for the separate reason that the Complaint nowhere alleges that Dechert was involved in the hacking. Based on either (or both) of these grounds, the Court should dismiss Plaintiff's CFAA claims. *Second*, Plaintiff's claim that Dechert participated in a conspiracy to violate the CFAA fails both because—as Judge Wang concluded—the Complaint does not allege a substantive violation of the CFAA, and also because it does not allege any facts that could lead to a reasonable inference that Dechert entered into an agreement to hack Plaintiff's emails. And *third*, Judge Wang rightly determined that all of Plaintiff's claims fail for the additional and independent reason that they were brought well beyond the applicable statute of limitations for both Plaintiff's state law conversion claim and his CFAA claims.

Plaintiff's Objections to Judge Wang's Report—which are as "incomprehensible" and "incoherent" as the other papers Judge Wang deemed as such, R&R 7 and 19—fail to rebut the compelling and thorough reasoning supporting Judge Wang's determination that all of Plaintiff's claims fail for multiple, independent reasons. His objections misconstrue the Report's reasoning without meaningfully addressing the many deficiencies with his Complaint. Accordingly, the Court should overrule Plaintiff's objections and dismiss the Complaint with prejudice.

PLAINTIFF'S ALLEGATIONS[2]

As noted above, this is the fourth litigation Plaintiff has filed in seven years stemming from his former role as Director and CEO of the RAK Free Trade Zone Authority ("RAKFTZA"), an instrumentality of RAK. *See* ECF No. 1 ("Complaint") ¶¶ 17–18 (describing two of the prior litigations). Two of the earlier litigations involved Dechert. In the first, Plaintiff brought claims in this District against RAKFTZA and related groups based on the alleged preparation of a "false smear report" that served as the pretext for his termination from his position at RAKFTZA. *Id.* ¶ 17. Dechert, through its former partner Linda Goldstein, represented RAKFTZA in that litigation. *Id*. Four years later, Plaintiff alleged that Dechert, former Dechert partner Neil Gerrard, and others had conspired to organize a "false smear campaign" against him. *Id.* ¶ 18. Dechert, again through Goldstein, represented itself and Gerrard in this second litigation. *Id.* Both prior litigations were dismissed at the pleading stage, and both dismissals were upheld on appeal. *Id.* ¶¶ 17–18.[3] Notably, in those prior litigations, Plaintiff also brought—and this Court rejected—claims under the CFAA. *See El Omari v. Buchanan*, 2021 WL 5889341, at *13 (S.D.N.Y. Dec. 10, 2021), *aff'd*, No. 22-55-CV, 2022 WL 4454536 (2d Cir. Sept. 26, 2022); *Omari v. Ras Al Khaimah Free Trade Zone Auth.*, 2017 WL 3896399, at *11 (S.D.N.Y. Aug. 18, 2017), *aff'd sub*

[2] On this motion, the well-pleaded allegations of the Complaint are assumed to be true. *McCarthy v. Dun & Bradstreet Corp.*, 482 F.3d 184, 191 (2d Cir. 2007). Dechert reserves all rights to—and does—dispute many of the allegations. Moreover, even on this motion, Defendants and the Court are "not required to credit conclusory allegations or legal conclusions couched as factual . . . allegations." *Id.*

[3] Plaintiff filed a third litigation in 2019 against the International Criminal Police Organization ("Interpol"), alleging that Interpol violated his rights as a result of his being scapegoated in a political conflict in RAK. *See Omari v. Int'l Crim. Police Org. – Interpol*, No. 19 CIV. 1457, ECF No. 1, ¶ 52 (E.D.N.Y. Mar. 13, 2019). That, too, was dismissed. *Omari v. Int'l Crim. Police Org. - Interpol*, 2021 WL 1924183, at *7 (E.D.N.Y. May 13, 2021), *aff'd*, 35 F.4th 83 (2d Cir. 2022), *cert. denied*, 143 S. Ct. 214 (2022). The Report does not note this litigation; it is mentioned here in the interest of completeness.

nom. El Omari v. Kreab (USA) Inc., 735 F. App'x 30 (2d Cir. 2018). Plaintiff refers to these two litigations together throughout his Complaint as the "NY Litigation." *See, e.g.*, Compl. ¶ 13. Plaintiff was represented in those litigations by his attorney in the present litigation. *Id.* ¶ 16.

I. Devices at Issue and the U.K. Litigation

Plaintiff alleges here that his email account was hacked on or about January 12, 2017 at the direction of a private investigator, Defendant Nicholas Del Rosso, and his company, Defendant Vital Management Services ("VMS"), that Dechert had previously engaged on its client's behalf. *Id.* ¶¶ 1, 20, 22. Plaintiff says he learned of this hacking in January 2023 when he received a "foreign notice pursuant to a U.K. court order." *Id.* ¶ 19. That notice informed him of the existence of three devices that are at issue in ongoing litigation in the U.K. *Id.* [4] One of those devices, a Huawei Matebook laptop ("the Laptop"), allegedly contains "a backup copy of emails containing the email address of El Omari's undersigned counsel (smm@milopc.com)." *Id.* ¶¶ 19–20. The emails allegedly include "communications between El Omari and his undersigned attorney," and their date range is said to encompass the period of the NY Litigation. *Id.* Neither of the other two devices is alleged to contain Plaintiff's emails.

II. Plaintiff's Investigation Into the Alleged Hacking

After receiving the "foreign notice," Plaintiff performed an investigation into the purported hacking. *Id.* ¶¶ 22–31. The investigation allegedly revealed that one of Plaintiff's email accounts—

[4] The U.K. proceedings in which the Laptop is at issue comprise (1) *Al Sadeq v. Dechert & Others*, Claim No. QB-2020-000322 ("Al Sadeq Proceedings"); (2) *Quzmar v. Dechert & Another*, QB-2020-003142 ("Quzmar Proceedings"); (3) *Stokoe Partnership v. Dechert & Another*, Claim No. QB-2020-002492 ("Stokoe Proceedings"); (4) *Mikadze & Massaad v. Dechert & Others*, Claim No. KB-2023-001629 ("Mikadze/Massaad Proceedings"); (5) *Ras al Khaimah Investment Authority v. Azima v. Dechert & Others*, Claim No. HC-2016-002798 ("Azima Proceedings"); (6) *Buchanan v. Stokoe*, Claim No. KB-2023-001629 ("Buchanan Proceedings"); and (7) *Del Rosso & Vital Management v. Stokoe*, Claim No. KB-2023-002877 ("Del Rosso Proceedings") (collectively, "the U.K. litigation"). Some of the U.K. litigation was commenced after the notice received by Plaintiff.

ceo@oussamaeelomari.com—was hacked "on or about January 12, 2017." *Id.* ¶ 22. Plaintiff infers that the email tranche found on the Laptop was copied from this account. *Id.* The investigation indicated that the hacking resulted from three phishing emails Plaintiff received in December 2016 and January 2017 to two of his email addresses. *Id.* ¶¶ 23, 31. Plaintiff opened and clicked on a link from someone he did not know; when the link did not open, his computer screen filled with "a page of computer language he did not understand." *Id.* ¶ 27. Plaintiff alleges this resulted in the acquisition of the credentials for Plaintiff's ceo@oussamaeelomari.com account, from which the hacker purportedly copied Plaintiff's emails. *Id.*

Based on nothing more than the alleged existence of his attorney's emails on the Laptop belonging to Del Rosso in 2023, Plaintiff speculates that the emails were "use[d] against him in the NY litigation" by providing "intelligence about El Omari's knowledge and information about the Ruler, legal positions, strategies, witnesses, evidence, and funding." *Id.* ¶¶ 13, 30. Plaintiff nowhere alleges the contents of any of the emails; how that content could have "assisted" Dechert in defending his claims (which, again, were dismissed at the pleading stage); nor even that the emails or their contents were ever actually provided to Dechert.

III. The Alleged Conspiracy

Plaintiff alleges that the hacking was performed by CyberRoot Risk Advisory Private Limited ("CyberRoot"), an Indian firm, and that CyberRoot was paid by Defendant Del Rosso to obtain Plaintiff's emails. *Id.* ¶¶ 7, 32. Del Rosso—via VMS's bank in North Carolina—purportedly sent "dozens of international wire transfers" totaling more than $500,000 to CyberRoot between July 2015—a year and a half before the alleged hacking—and December 2016. *Id.* ¶¶ 33–34.

Apparently based on these payments to CyberRoot, and Del Rosso's engagement by Dechert, Plaintiff alleges that Dechert, Del Rosso, and VMS conspired with others, including CyberRoot, "to hack and access confidential emails of El Omari, and other Dechert LLP's

litigation adversaries." *Id.* ¶ 36. Del Rosso, Plaintiff alleges, had "actual knowledge of the illegal activities." *Id.* ¶ 37. And Dechert, Plaintiff speculates, "either had actual knowledge, or must have strongly suspected the illegal hacking activities of its private investigator Del Rosso and CyberRoot." *Id.* ¶ 38. That is purportedly because the money paid by Del Rosso to CyberRoot was "in turn costs to Dechert," and the information allegedly revealed in the confidential emails "must have triggered strong suspicions by Goldstein," Dechert's former partner and counsel in Plaintiff's previously dismissed cases. *Id.* ¶ 38. Goldstein, Plaintiff alleges, "must have deliberately avoided learning about the illegal sourcing of the sensitive information." *Id.* Plaintiff never alleges, however, that Goldstein entered into any agreement with Del Rosso or others regarding the hacking, or that she, or anyone at Dechert, directed, encouraged, or paid for it. *Id.* Nor does he allege, again, that the emails were provided to Goldstein or anyone else at Dechert. *Id.*

IV. Plaintiff's Claims

As a result of the unauthorized access of his emails, Plaintiff allegedly suffered "injuries to his business and property." *Id.* ¶ 42. He asserts that his damages "are in excess of tens of thousands of dollars paid to date in legal fees and costs, and forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to remedy the complete loss of the confidentiality of the emails." *Id.* ¶ 41.

On the basis of the foregoing, Plaintiff alleges that Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C) (Count I); conspired to commit the same, in violation of 18 U.S.C. § 1030(b) (Count II); and committed conversion under the common law of North Carolina (Count III). Compl. ¶¶ 47–75.

STANDARD OF REVIEW

Federal Rule of Civil Procedure 12(b)(6) requires that a complaint "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v.*

Iqbal, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A court first reviews plaintiff's complaint "to identify allegations that, 'because they are no more than conclusions are not entitled to the assumption of truth'"; it then considers whether the "remaining well-pleaded factual allegations … 'plausibly give rise to an entitlement to relief.'" *Reis, Inc. v. Lennar Corp.*, 2016 WL 3702736, at *3 (S.D.N.Y. July 5, 2016) (quoting *Iqbal*, 556 U.S. at 679).

A district court must conduct a "*de novo* review of those portions of [a Magistrate's] report ... to which timely objections are made." *Terio v. Michaud*, 2011 WL 868661, at *1 (S.D.N.Y. March 10, 2011) (citing 28 U.S.C. § 636(b)(1)). However, "[t]o the extent ... that the party makes only conclusory or general arguments, or simply reiterates the original arguments, the Court will review the Report strictly for clear error." *Id.* (citing *IndyMac Bank, F.S.B. v. Natl. Settlement Agency, Inc.,* 2008 WL 4810043, at * 1 (S.D.N.Y. Nov. 3, 2008)); *see also New York City District Council of Carpenters Pension Fund v. Forde*, 341 F. Supp. 3d 334, 337 (S.D.N.Y. 2018) (applying "clear error" review where arguments were simple "rehash" of arguments before Magistrate). Here, Plaintiff largely re-hashes the same arguments made before Judge Wang, and therefore clear error review is appropriate; under any standard, however, dismissal is warranted.

ARGUMENT

Plaintiff brings two causes of action under the CFAA, and one under North Carolina common law. As Judge Wang correctly concluded, the Complaint fails to state a claim on all three. *First*, the Report found that the CFAA claims should be dismissed because Plaintiff fails to plead a cognizable "damage" or "loss" as required by the statute and binding precedent. Specifically, Plaintiff's claims for losses concerning attorneys' fees and costs and the loss of the confidentiality in his emails are not cognizable losses under the CFAA. And although Plaintiff claims a loss

relating to the forensic investigation he conducted following awareness of the hacking, as Judge Wang determined, the Complaint nowhere alleges that the investigation sought to identify and remedy a *technological harm* caused by the hacking, nor does it specify the amount of loss attributable to that investigation, both of which are requirements under the CFAA. Judge Wang also correctly concluded that Plaintiff's CFAA claims should be dismissed for the additional reason that Plaintiff fails to allege that Dechert itself played a role in violating the statute—a fatal flaw in his CFAA claim that Plaintiff has made in past unsuccessful attempts to litigate CFAA claims against other parties. *Second*, the CFAA conspiracy claim must be dismissed for the additional reason that the allegations of conspiracy are conclusory and insufficient to state a claim for relief that is plausible on its face. *Finally*, as Judge Wang rightly determined, all of Plaintiff's claims are time barred and should be dismissed on that ground as well.

I. Judge Wang Properly Concluded that the Complaint Fails to State a Claim Under the CFAA

The Report correctly concluded that the Complaint fails to state a claim under the CFAA. As noted above, in his past litigations, Plaintiff has twice tried, and twice failed, to bring CFAA claims. His claims fare no better here. As Judge Wang found, Plaintiff's CFAA claims are deficient on two independent grounds: (1) Plaintiff failed to allege actionable losses under the CFAA; and (2) Plaintiff failed to allege any involvement by Dechert (or co-Defendants) in the hacking of his emails. His CFAA claims should be dismissed for either (or both) of these reasons.

A. The Complaint Fails to Plead Actionable "Loss" Under the CFAA

As Judge Wang concluded, Plaintiff's CFAA claims should be dismissed because he failed to plead an actionable "loss" under the CFAA. R&R at 18–20. To sustain a claim under the CFAA, a plaintiff must allege "damage" or "loss" that falls within the CFAA's narrow definition of those terms. *See, e.g.*, *Dreni v. PrinterOn Am. Corp.*, 486 F. Supp. 3d 712, 735-36 (S.D.N.Y. 2020). The

CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). And it defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11).

Courts have interpreted both terms narrowly. Just two years ago, the Supreme Court clarified that the CFAA's "damage" and "loss" "focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data." *Van Buren*, 141 S. Ct. at 1660. Such an interpretation "makes sense in a scheme 'aimed at preventing the typical consequences of hacking.'" *Id.* (citation omitted). And indeed, "[b]oth before and after the Supreme Court's decision in *Van Buren*, 'courts in this District [have] interpreted the CFAA to require loss related to damage or impairment of the target computer itself.'" *Rekor Sys., Inc. v. Loughlin*, 2022 WL 789157, at *11 (S.D.N.Y. Mar. 14, 2022) (quoting *El Omari v. Buchanan*, 2021 WL 5889341, at *14 (S.D.N.Y. Dec. 10, 2021)). Only such "technological harms" damages or losses count towards satisfying the $5,000 threshold. *See Dreni*, 486 F. Supp. 3d at 736–37 (excising unrecoverable losses in assessing whether threshold met).

Judge Wang correctly concluded that Plaintiff did not plead costs that were "compensable under" the CFAA. R&R at 19–20. Plaintiff alleges three forms of loss: (1) "legal fees and costs," Compl. ¶ 50; (2) "forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to restore the complete loss of the confidentiality of the emails," *id.*; and (3) "loss of the valuable confidentiality of the data in the attorney-client communication emails which relate to El Omari's NY litigation," *id.* ¶ 52. As Judge Wang found, all three of these

"vague and conclusory" harms are "insufficient" under the CFAA. R&R at 18.

With respect to the first and third categories of "loss" that Plaintiff alleges—legal fees and "loss of valuable confidentiality"—Judge Wang properly concluded that these "general," "conclusory," and "incoherent[]" theories of loss fall outside the scope of CFAA. R&R at 18–19. Even before *Van Buren*, CFAA losses were limited to "remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made," and thus costs that are several steps removed from the accessed computer may not be recovered. *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474–76 (S.D.N.Y. 2004), *aff'd*, 166 F. App'x 559 (2d Cir. 2006). As a result, and as a rule, "litigation-related expenses do not qualify as 'losses' under the CFAA." *Dreni*, 486 F. Supp. 3d at 736 (collecting cases); *see also Goodman v. Goodman*, 2022 WL 17826390, at *9 (S.D.N.Y. Dec. 21, 2022), *report and recommendation adopted*, 2023 WL 1967577 (S.D.N.Y. Feb. 12, 2023) (collecting cases holding the same after *Van Buren*). Nor do non-economic losses like "loss of the confidentiality" of emails. Compl. ¶ 52; *see Jensen v. Cablevision Sys. Corp.*, 2017 WL 4325829, at *13 (E.D.N.Y. Sept. 27, 2017) (finding "invasion of . . . privacy" not a cognizable loss under CFAA). Plaintiffs' first and third forms of loss are therefore easily disposed.

Plaintiff's second category of loss—the "forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to restore the complete loss of the confidentiality of the emails," Compl. ¶ 50—also fails to plead a cognizable "loss" under the CFAA, for two reasons. *First*, as Judge Wang rightly found, Plaintiff "does not sufficiently allege that the[se] costs … were 'from efforts to identify, diagnose, or address'" any technological harm that is recoverable under the CFAA. R&R at 19. Insofar as "the costs of investigating security breaches constitute recoverable 'losses,'" *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F.

Supp. 2d 378, 387 (S.D.N.Y. 2010), that is so *only* when the investigation is performed "to identify, investigate, or remedy any *covered damage*," *Better Holdco, Inc. v. Beeline Loans, Inc.*, 2021 WL 3173736, at *4 (S.D.N.Y. July 26, 2021) (emphasis added). And "covered damage," as the Supreme Court, the Second Circuit, and courts in this District have interpreted that term under CFAA, includes only technological harm. *Id.*; *see also Van Buren*, 141 S. Ct. at 1660. As a court in this District already explained in rejecting one of Plaintiff's prior shots at a CFAA claim, "the focus is on the connection between the plaintiff's response and 'damage to or impairment of the protected computer.'" *Buchanan*, 2021 WL 5889341, at *14 (citing *Better Holdco, Inc.*, 2021 WL 3173736, at *3).

Here, Plaintiff alleges vaguely that he initiated "an investigation to determine what email account was hacked to obtain the stolen email tranche." Compl. ¶ 22. As Judge Wang noted, this investigation into "the *scope* of the hacking," R&R at 18 (emphasis added), does not allege that the investigation sought to identify or assess the requisite technological harm to the computer or its information. Instead, Plaintiff alleges only that the investigation was aimed at "seeking to restore the complete loss of the confidentiality of the emails." *Id.* ¶ 50. But as Judge Wang properly concluded, and as this Court has repeatedly held, the investigation into the downloading and copying of emails is "not compensable" under the CFAA. R&R at 19; *see also Better Holdco, Inc.*, 2021 WL 3173736, at *4 (finding allegation that data was downloaded and copied did not plead technological harm, and investigation into extent of misappropriation of confidential information was not covered loss); *Reis*, 2016 WL 3702736, at *6 (where plaintiff alleged he "expend[ed] time, money, and resources … to conduct an investigation into the intrusion and a damages assessment," CFAA claim insufficient absent "allegations that the investigation was for the purpose of looking into any damage to data, programs, or server system"); *Fink v. Time Warner Cable*, 810 F. Supp.

2d 633, 641 (S.D.N.Y. 2011), *on reconsideration*, 2011 WL 5121068 (S.D.N.Y. Oct. 28, 2011) (allegations of losses "relating to time and effort in assessing 'damage' to each computer" failed because they did not allege loss relating to remedying damage or restoring data). Simply put, despite having been warned by the Court in his previously-dismissed Complaints that his CFAA claims would fail absent an allegation of "damage to or impairment of the protected computer," *Buchanan*, 2021 WL 5889341, at *14, Plaintiff once again falls well short here.

Second, even *if* Plaintiff had sufficiently alleged damage or loss related to the "forensic computer investigation costs," the Complaint fails to break down which portion of his expenses are attributable to those costs rather than, for example, inapplicable attorney's fees. *See* Compl. ¶ 54 (alleging one-year loss "in excess of $5,000 expended in forensic computer investigation costs and attorney fees in this proceeding"). Courts have found that these sorts of insufficiently specific loss allegations are fatal to a CFAA claim. *See Reis*, 2016 WL 3702736, at *7; *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 514 (S.D.N.Y. 2015). While Plaintiff asserts in his Objections that the Complaint pleads "forensic computer investigation costs in excess of $5,000," Obj. at 15–16, it does no such thing. *See, e.g.*, Compl. ¶ 41.

Plaintiff says that Judge Wang "improperly rewrote the complaint" by purportedly concluding that some of these "costs were really incurred in prior cases bringing the costs [in this case] to a level below $5,000." Obj. at 16. Not so. Plaintiff bases this argument on only a footnote in which Judge Wang expressed confusion at what exactly Plaintiff included in his "forensic computer investigation costs," given the vague and conclusory language in the Complaint. R&R at 18, n.24. It is, in fact, Plaintiff who attempts to rewrite the R&R, and fails to rebut Judge Wang's conclusion that none of Plaintiff's alleged costs "were 'from efforts to identify, diagnose, or address'" technological harm. R&R at 19 (citation omitted).

Plaintiff also insists that Judge Wang incorrectly applied *Van Buren* in concluding that Plaintiff's alleged costs in "restoring" his confidentiality are not compensable under the CFAA. Obj. at 17–20. But Plaintiff does not challenge Judge Wang's conclusion that, under *Van Buren*, "the 'loss of privilege of' Plaintiff's emails is *not* recoverable damage." R&R at 20, n.26. Instead, Plaintiff takes issue with Judge Wang's application of *Van Buren*, based on the mistaken premise that Judge Wang concluded that Plaintiff's database was "harmed." Obj. at 20. But, again, Plaintiff misreads the R&R. Judge Wang did not conclude that some database belonging to Plaintiff was harmed. Plaintiff quotes from the portion of the R&R where Judge Wang says only that Plaintiff had been "hacked by someone." Obj. at 20. Such unauthorized access alone is not technological harm—that is the point of *Van Buren* and the line of authorities which it built construing cognizable loss under the CFAA.

B. The Complaint Fails to Plead Dechert's Involvement

The Report also correctly concluded that Plaintiff's CFAA claims fail for the additional reason that "Plaintiff does not allege that any Defendant accessed his computer, nor that any Defendant was affiliated with the hack." R&R at 16. To state a claim under Section 1030(a)(2)(c) of the CFAA, Plaintiff must plead that Dechert "intentionally access[ed] a computer without authorization." *Id.* As Judge Wang found, Plaintiff has not done so. While Plaintiff alleges that Dechert "either had actual knowledge, or must have strongly suspected the illegal hacking activities," Compl. ¶ 38, Judge Wang correctly noted that "Plaintiff still does not plead facts to establish that Defendants … hacked or conspired to hack his emails," R&R at 17. As courts in this District have recognized time and again, CFAA claims cannot lie where "Plaintiff has provided no facts to establish that [Defendant] is affiliated with the hack[] of Plaintiffs' computers." *Broidy v. Glob. Risk Advisors LLC*, 2021 WL 1225949, at *9 (S.D.N.Y. Mar. 31, 2021); *see also JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 526 (S.D.N.Y. 2013) (dismissing CFAA

claim at pleading stage where plaintiff asserted only "speculative" allegations that defendants had hacked server).

Plaintiff has committed this same pleading failure twice previously. In *RAKFTZA*, this Court rejected his CFAA claim because "plaintiff does not allege sufficient factual matter to permit a 'reasonable inference' that RAKFTZA—as opposed to someone else—was involved in the hacking of plaintiff's website." 2017 WL 3896399, at *11. And in *Buchanan*, this Court again dismissed Plaintiff's CFAA claim because "El Omari fails to plausibly allege that Defendants—as opposed to someone else—were responsible for any purported hacking of El Omari's computer or conspired … for that purpose." *Buchanan*, 2021 WL 5889341, at *13. Plaintiff's third swing misses the pitch again.

Plaintiff again incorrectly contends that Judge Wang "erroneously rewrote the complaint." Obj. at 12. But in fact, Judge Wang considered each of Plaintiff's allegations and correctly concluded that Plaintiff failed to tie Dechert to any hacking of Plaintiff's email. R&R at 17–18. As Judge Wang described, Plaintiff merely alleged that he was hacked by *someone*, that Defendant Vital had made payments to non-parties in India, and that his emails ultimately ended up on Defendant Vital's computer. *Id.* These are insufficient to draw a connection of hacking to Defendant Vital, let alone Dechert. *id.* at 18 ("[T]here is no connection drawn between Defendants and any hacker or hacking activity…."). Simply put, Dechert's involvement in Plaintiff's hacking is "not [a] plausible inference[] to draw" from Plaintiff's conclusory and vague allegations. *Id.* at 17.

II. Judge Wang Properly Concluded that the Complaint Failed to Plead a Claim for Conspiracy to Violate the CFAA

Plaintiff fails to object to Judge Wang's finding that Plaintiff did not sufficiently plead conspiracy. Accordingly, the Court reviews the Report on this score for clear error only. *Henry v.*

United States, 346 F. Supp. 2d 496, 496 (S.D.N.Y. 2004). Because Judge Wang correctly held that there was no allegation of a conspiracy, there was no clear error.

To start, because Plaintiff failed to plead a substantive violation of the CFAA, he has also failed to plead a claim for conspiracy to violate that statute under 18 U.S.C. § 1030(b). *See Espire Ads LLC v. TAPP Influencers Corp.*, 2023 WL 1968025, at *15 (S.D.N.Y. Feb. 13, 2023); *Reis*, 2016 WL 3702736, at *7 (citing *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 836 (N.D. Cal. 2014), and *PNC Mortgage v. Superior Mortgage Corp.*, 2012 WL 627995, at *4 (E.D. Pa. Feb. 27, 2012)).

But even if Plaintiff had adequately pleaded a threshold violation of the CFAA, his conspiracy claim against Dechert would still fail. Conspiracy claims require "specific allegations of an agreement and common activities" among co-conspirators. *NetApp, Inc.*, 41 F. Supp. 3d at 835–36 (collecting cases). Specifically, "to survive a motion to dismiss, plaintiff must allege with sufficient factual particularity that defendants reached some explicit or tacit understanding or agreement." *Id.* at 836 (cleaned up).

Judge Wang correctly determined that "Plaintiff … [has] not plead[ed] facts to establish that Defendants … conspired to hack his emails." R&R at 17. As noted above, the only allegations Plaintiff levies with regard to Dechert as it concerns the alleged hacking is that "Dechert LLP either had actual knowledge, or must have strongly suspected the illegal hacking activities of its private investigator Del Rosso and CyberRoot." Compl. ¶ 38. Plaintiff does not allege that Dechert directed Del Rosso to hire CyberRoot, or came to any agreement with Del Rosso to do so. Although Plaintiff muses that the "sharing of the sensitive information gleaned from the stolen confidential emails with Goldstein at Dechert NY must have triggered strong suspicions by Goldstein, an experienced and learned law professional, that El Omari's sensitive litigation information was

illegally obtained," *id.*, the Complaint does not actually allege that Goldstein or Dechert were in fact provided with any of the supposedly hacked data or emails, let alone that they agreed with others to hack the data or otherwise access Plaintiff's emails in the first place. And although Plaintiff contends that Defendants Del Rosso and VMS paid CyberRoot over $500,000 from July 2015 to December 2016 and that these were "in turn costs to Dechert," the Complaint never alleges any facts to support Plaintiff's conjecture that the money was coming from Dechert, and even if it did, the Complaint does not allege that the supposed "costs" would have been identifiable as having anything to do with hacking. *Id.* In short, the Complaint fails to allege the requisite agreement.

III. Judge Wang Properly Concluded that All of Plaintiff's Claims Are Time Barred

The Report also correctly found that all of Plaintiff's claims are time barred. Plaintiff brought this action six years after the alleged hacking in 2017. Plaintiff's conversion claim is thus clearly time barred under North Carolina's three-year statute of limitations. Moreover, Plaintiff's CFAA claims—which fail for the independent reasons set forth above—likewise fail under that statute's two-year statute of limitations.

A. Plaintiff's Conversion Claim is Time-Barred

Conversion claims are subject to a three-year statute of limitations in North Carolina. *See* N.C. Gen. Stat. § 1–52(4); *see also Honeycutt v. Weaver*, 257 N.C. App. 599, 609 (2018). The "discovery rule" does not apply to conversion claims under North Carolina law because N.C. Gen. Stat. § 1–52(4) does not contain language providing for one, as do other subsections of Gen. Stat. § 1–52. *See White v. Consol. Plan., Inc.*, 166 N.C. App. 283, 310 (2004). Thus, a conversion claim "accrues, and the statute of limitations begins to run, when the unauthorized assumption and exercise of ownership occurs—not when the plaintiff discovers the conversion." *Stratton v. Royal Bank of Canada*, 211 N.C. App. 78, 83 (2011). The statute of limitations for Plaintiff's CFAA claims is two-years. 18 U.S.C. § 1030(g).

As Judge Wang rightly concluded, Plaintiff's conversion claim accrued "in 2017, more than six years before this action was commenced." R&R at 12. His conversion claim is thus time barred. *See Ferro v. Vol Vo Penta of the Americas, LLC*, 2017 WL 3710071, at *4 (E.D.N.C. Aug. 28, 2017), *aff'd sub nom. Ferro v. Volvo Penta of the Americas, LLC*, 731 F. App'x 208 (4th Cir. 2018) (applying North Carolina law and concluding conversion claim time barred when "conversion occurred more than three years before the filing of [plaintiff's] complaint").

Plaintiff claims that Judge Wang "did not consider application of the discovery rule under more recent case law," Obj. at 21, but he points to no case law establishing that the discovery rule applies to *conversion claims*, where North Carolina courts have said the opposite. *See Stratton*, 211 N.C. App. at 83. Plaintiff's sole case applies the discovery rule to breach of contract claims, not conversion claims. *See* Obj. at 21 (quoting *Chisum v. Campagna*, 855 S.E.2d 173, 188-89 (N.C. 2021)). Plaintiff offers no explanation why this Court should reject binding North Carolina precedent and adopt a new rule applicable to a different claim, contrary to statute and jurisprudence. Judge Wang rightly applied North Carolina law to reject application of the discovery rule to Plaintiff's conversion claim.

Plaintiff also asserts that Judge Wang failed to consider his argument that his conversion claim did not accrue until 2023 when he discovered that his emails were on the Laptop, because he "could not be excluded from the subject emails if he didn't know they were on the Laptop." Obj. at 21. This rather incomprehensible argument is just a re-formulation of his discovery rule argument and should be rejected for the same reason—there is no discovery rule for conversion claims. Even if merely copying emails constituted conversion,[5] Plaintiff's supposed dominion over

[5] Judge Wang also correctly concluded that the hacking of Plaintiff's emails fails to state a claim of conversion because "[e]mails are neither goods nor personal chattels, and Plaintiff's use of his

the emails was allegedly violated as soon as they left his inbox and someone else could direct their use. *See Bridgetree, Inc. v. Red F Mktg. LLC*, 2013 WL 443698, at *15 (W.D.N.C. Feb. 5, 2013) (finding deprivation of plaintiff's exclusive control over electronically-stored proprietary information constituted conversion, with no consideration for plaintiff's knowledge of deprivation). Any other rule would create a special discovery rule for conversion of electronic files, which is not supported by the statute or relevant precedent.

Finally, Plaintiff argues that Judge Wang mistakenly rejected Plaintiff's equitable estoppel argument, but Judge Wang correctly found that Plaintiff inadequately pleaded equitable estoppel. Equitable estoppel is only appropriate when certain conditions are present—namely, "(1) conduct on the part of the party sought to be estopped which amounts to a false representation or concealment of material facts; (2) the intention that such conduct will be acted on by the other party; and (3) knowledge, actual or constructive, of the real facts." *Friedland v. Gales*, 131 N.C. App. 802, 807 (Ct. App. 1998) (citations omitted). "The party asserting the defense must have (1) a lack of knowledge and the means of knowledge as to the real facts in question; and (2) relied upon the conduct of the party sought to be estopped to his prejudice." *Id.* A party seeking to invoke the doctrine of equitable estoppel "must plead the facts with particularity, demonstrating that it was the defendant's representations which delayed it from filing suit." *N.C. State Bar v. Gilbert*, 2006 WL 539367, at *4 (N.C. Ct. App. Mar. 7, 2006).

---

email account apparently continued unimpeded." R&R at 20 (internal footnote omitted). A "growing body" of North Carolina case law holds that making copies of electronically stored information does not support claim for conversion. *Addison Whitney, LLC v. Cashion*, 2017 WL 2506604, at *7 (N.C. Super. June 9, 2017). Plaintiff responds by repeatedly asserting that the hacking "violated Plaintiff's dominion or control over" his emails, but he does not dispute that his access to his email was not impeded. This provides yet another basis for dismissing that claim.

As Judge Wang found, "[o]ther than conclusory assertions in his opposition, Plaintiff has not pleaded" equitable estoppel, including the required elements of "conduct, intent, or knowledge of the real facts." R&R at 13, n.19. Plaintiff points only to the conclusory allegations underlying his conversion claim, *see* Obj. at 11–12, conceding that he has not "specifically pled" estoppel, or any of its elements. *Eastpointe Hum. Servs. v. N. C. Dep't of Health & Hum. Servs.*, 2022 WL 2439157, at *9 (N.C. Ct. App. July 5, 2022). That is fatal to his claim.

B. Plaintiff's CFAA Claims Are Time Barred

Likewise, the Report properly determined that Plaintiff's CFAA claims should be dismissed as time barred. As Judge Wang found, "Plaintiff discovered the intrusion in January 2017, as soon as he clicked on the link—which was embedded in an attachment that was attached to an email sent from someone he did not know—when the link did not open, and his computer screen filled with 'a page of computer language he did not understand.'" R&R at 12. Plaintiff thus "discovered" his purported injury for CFAA purposes "in 2017," and brought this claim in 2023, well beyond the two-year statute of limitations. *Id.*

Plaintiff contends that Judge Wang misconstrued the facts in concluding the CFAA claims accrued in 2017, but fails to rebut the Report's reasoning. Plaintiff does not dispute the Complaint alleges that when he clicked the phishing link that allegedly led to his hacking, Plaintiff saw "a page of computer language he did not understand," *id*. ¶ 27. Nor does Plaintiff dispute that, at that time, he was familiar with computer hacking (given his repeated litigations on the subject), nor does he argue that he could not reasonably have been on notice that he had been hacked. Based on these undisputed facts, Judge Wang concluded, relying on *Sewell v. Bernardin*, 795 F.3d 337 (2d Cir. 2015), that it would be implausible to believe Plaintiff's theory that he only discovered the damage in 2023. R&R at 12. In *Sewell*, the panel held that a CFAA claim began to run as soon the plaintiff could not log in to her AOL account; "[t]hat she may not have known exactly what

happened or why she could not log in is of no moment." 795 F.3d at 340. Here, the statute of limitations began as soon as Plaintiff "clicked on the link—which was embedded in an attachment that was attached to an email sent from someone he did not know—when the link did not open, and his computer screen filled with 'a page of computer language he did not understand.'" R&R at 12; *see also Verschleiser v. Frydman*, 2023 WL 5835031, at *8 (S.D.N.Y. Sept. 7, 2023) (finding CFAA claims untimely where results of hacking would have been apparent years previously).

Plaintiff also contends that Judge Wang erroneously dismissed his CFAA claims based on "that portion of the hacked email tranche on Del Rosso's Laptop which fall[s]" after 2017. Obj. at 10. But the Complaint alleges only that the hacking of Plaintiff's email "occurred on or about January 12, 2017." Compl. ¶ 20. It does not allege that there were future hacks of Plaintiff's email; as relevant, it alleges only that the Laptop file which contained Plaintiff's emails also contained data "determined to be between March 2011 and May 2021." *Id.* Judge Wang thus correctly concluded that Plaintiff pleaded that he was hacked in 2017, that he discovered his purported injury at that time, and therefore his CFAA claims are untimely.

CONCLUSION

For the foregoing reasons, Dechert respectfully requests that the Court adopt Magistrate Judge Wang's Report and Recommendation.[6]

[6] Plaintiff also objects to Judge Wang's disposition of his motion for a preliminary injunction. However, as Plaintiff notes, he and Dechert "resolved the motion for preliminary injunction as to Dechert by stipulation." Obj. at 1, n.1. This "mooted" the preliminary injunction as to Dechert. R&R at 6.

Dated: March 21, 2024
New York, New York

By: 

Sean Hecker
John C. Quinn
David Gopstein
Mark Weiner
KAPLAN HECKER & FINK LLP
350 Fifth Avenue, 63rd Floor
New York, NY 10118
Tel: (212) 763-0883
Fax: (212) 564-0883
shecker@kaplanhecker.com
jquinn@kaplanhecker.com
dgopstein@kaplanhecker.com
mweiner@kaplanhecker.com

Carmen Iguina González*
KAPLAN HECKER & FINK LLP
1050 K Street NW, Suite 1040
Washington, DC 20001
Tel: (212) 763-0883
Fax: (212) 564-0883
ciguinagonzalez@kaplanhecker.com

Attorneys for Defendant Dechert LLP

**Admitted pro hac vice*